

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

TERRENCE J. WHITE,	)	
	)	
Plaintiff,	)	
	)	
v.	)	CIVIL ACTION
	)	FILE NO. 1:09-cv-00151-WSD
THURBERT E. BAKER, et al.,	)	
	)	
Defendants.	)	

**MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S  
MOTION FOR PRELIMINARY AND PERMANENT INJUNCTION  
AND DECLARATORY RELIEF**

Emmet J. Bondurant  
Georgia Bar No. 066900  
Nicole G. Iannarone  
Georgia Bar No. 382510  
Elizabeth G. Eager  
Georgia Bar No. 644007  
Bondurant, Mixson & Elmore, LLP  
Attorneys at Law  
3900 One Atlantic Center  
1201 West Peachtree Street, NW  
Atlanta, Georgia 30309-3417  
Phone: 404-881-4100  
Facsimile: 404-881-4111  
krugman@bmelaw.com  
eager@bmelaw.com

## **TABLE OF CONTENTS**

FACTUAL BACKGROUND AND SUMMARY OF THE ARGUMENT .....	1
ARGUMENT AND CITATION OF AUTHORITY .....	4
I. Plaintiff Will Succeed On The Merits Of His Claims .....	5
A. The E-Information Provisions Are Preempted .....	5
1. The SCA Preempts The Stored Communications Field .....	7
2. The E-Information Provisions Conflict With The SCA .....	8
B. The Provisions Violate First Amendment Free Speech Rights .....	9
1. The Provisions Violate The Right to Anonymous Speech .....	9
2. The Provisions Are Presumptively Invalid Content-Based Restrictions .....	10
3. The E-Information Provisions Are A Prior Restraint .....	13
4. The E-Information Provisions Are Overly Broad .....	14
5. The E-Information Provisions Are Void For Vagueness .....	15

C.	The E-Information Provisions Infringe Private Association.....	15
D.	The E-Information Provisions Violate The Fourth Amendment .....	17
1.	The Fourth Amendment Bars Searches Without A Warrant .....	17
2.	The E-Information Provisions Are A Constructive Seizure .....	20
E.	E-Information Provisions Are An Ex Post Facto Law .....	22
II.	Plaintiff Faces A Substantial Threat of Irreparable Injury.....	23
III.	The Balance of Hardships Weighs In Plaintiff's Favor .....	24
IV.	The Issuance Of An Injunction Promotes the Public Interest .....	24

## **TABLE OF AUTHORITIES**

<i>ACLU v. Miller</i> , 977 F. Supp. 1228 (N.D. Ga. 1997).....	10, 11, 14, 15, 24, 25
<i>Ashcroft v. ACLU</i> , 542 U.S. 656 (2004) .....	10, 11, 12
<i>Bansal v. Russ</i> , 513 F. Supp. 2d 264 (E.D. Pa. 2007) .....	6
<i>Bates v. City of Little Rock</i> , 361 U.S. 516 (1960).....	16, 17
<i>Bourgeois v. Peters</i> , 387 F.3d 1303 (11 <sup>th</sup> Cir. 2004).....	13
<i>Bunnell v. Motion Picture Assn. of America</i> , 567 F. Supp. 2d 1148 (C.D. Cal. 2007) .....	7
<i>Cardinal Health 414, Inc. v. Adams</i> , 582 F. Supp. 2d 967 (M.D. Tenn. 2008).....	6
<i>Cliff v. Payco Gen. Am. Credits Inc.</i> , 363 F.3d 1113 (11 <sup>th</sup> Cir. 2004).....	5, 7, 8
<i>Doe v. Miller</i> , 405 F.3d 700 (8 <sup>th</sup> Cir. 2005) .....	23
<i>Doe v. Prosecutor, Marion County, Ind.</i> , 566 F. Supp. 2d 862 (S.D. Ind. 2008) .....	4, 19, 20
<i>Doe v. Shurtleff</i> , No. 1:08-cv-64, 2008 WL 4427594 (D. Utah Sept. 25, 2008).....	4, 9, 10, 12
<i>Doe v. 2TheMart.com Inc.</i> , 140 F. Supp. 2d 1088 (W.D. Wash. 2001).....	10
<i>Gibson v. Florida Legislative Committee</i> , 372 U.S. 539 (1963).....	16, 17
<i>KH Outdoor, LLC. v. Trussville</i> , 458 F.3d 1261 (11 <sup>th</sup> Cir. 2006).....	5, 24, 25
<i>Kansas v. Hendricks</i> , 521 U.S. 346 (1997).....	23

<i>Katz v. U.S.</i> , 389 U.S. 347 (1967).....	17, 19
<i>Kennedy v. Mendoza-Martinez</i> , 372 U.S.144 (1963) .....	23
<i>Maryland v. Macon</i> , 472 U.S. 463 (1985).....	18, 20
<i>McIntyre v. Ohio Elections Comm’n</i> , 514 U.S. 334 (1995) .....	10
<i>Muskovich v. Crowell</i> , No. 3-95-CV-80007, 1995 WL 905403 (S.D. Iowa March 21, 1995).....	7
<i>NAACP v. Alabama ex rel. Patterson</i> , 357 U.S. 449 (1958) .....	16
<i>New York v. P.J. Video, Inc.</i> , 475 U.S. 868 (1986).....	20
<i>Northeastern Fla. Chapter of the Assn. of Gen. Contractors of America v. City of U.S. v. Councilman</i> , 418 F.3d 67 (1 <sup>st</sup> Cir. 2005).....	24
<i>Penthouse Int’l, Ltd. v. McAuliffe</i> , 610 F.2d 1353 (11 <sup>th</sup> Cir. 1980).....	20, 21
<i>Provident Mut. Life Ins. Co. v. Atlanta</i> , 864 F.Supp. 1274 (N.D. Ga. 1994) .....	13
<i>Pure Power Boot Camp v. Warrior Fitness Boot Camp</i> , 587 F. Supp. 2d 548 (S.D.N.Y. 2008) .....	5, 6
<i>Quon v. Arch Wireless Operating Co.</i> , 445 F. Supp. 2d at 1116 (C.D. Cal. 2006).....	7, 18, 19
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	10, 11, 15

<i>Retail Clerks Int’l Ass’n, Local 1625 v. Schermerhorn</i> , 375 U.S. 96 (1963).....	7
<i>Rodan v. Kentucky</i> , 413 U.S. 496 (1973).....	21
<i>Sable Comms. of Ca., Inc. v. FCC</i> , 492 U.S. 115 (1989) .....	11
<i>Sinclair v. TubeSockedD</i> , 596 F. Supp. 2d 128 (D.D.C. 2009) .....	10
<i>Smith v. Doe</i> , 538 U.S. 84 (2002) .....	22, 23
<i>Solantic v. City of Neptune Beach</i> , 410 F.3d 1250 (11 <sup>th</sup> Cir. 2005).....	10
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	19
<i>U.S. v. Councilman</i> , 418 F.3d 67 (1 <sup>st</sup> Cir. 2005) .....	6
<i>U.S. v. Finley</i> , 477 F.3d 250 (5 <sup>th</sup> Cir. 2007).....	18
<i>U.S. v. Forrester</i> , 512 F.3d 500 (9 <sup>th</sup> Cir. 2008) .....	18
<i>U.S. v. Jacobsen</i> , 466 U.S. 109 (1984) .....	20
<i>U.S. v. Mitchell</i> , ___ F.3d ___, 2009 WL 1067212 (11 <sup>th</sup> Cir. Apr. 22, 2009) .....	21
<i>U.S. v. Steiger</i> , 318 F.3d 1039 (11 <sup>th</sup> Cir. 2003) .....	6
<i>Watchtower Bible &amp; Tract Soc’y of N.Y. v. Village of Stratton</i> , 536 U.S. 150 (2002) .....	10

## **STATUTES**

O.C.G.A. § 16-6-5.....	<i>passim</i>
O.C.G.A. § 42-1-12.....	<i>passim</i>
18 U.S.C. § 2701 .....	<i>passim</i>
18 U.S.C. § 2702.....	<i>passim</i>
18 U.S.C. § 2703.....	<i>passim</i>
18 U.S.C. § 2704.....	<i>passim</i>
18 U.S.C. § 2707.....	<i>passim</i>
18 U.S.C. § 2708.....	<i>passim</i>

## **OTHER**

2008 Ga. Laws p. 810 (“SB 474”) .....	2
Model Internet Safety Legislation Passes Senate, Press Release from Georgia State Senator Cecil Stanton, February 28, 2008 .....	2, 6, 8, 9, 18, 22
Andrew Schrock & Danah Boyd, Online Threats to Youth: Solicitation, Harassment, and Problematic Content: Literature Review Prepared for the Internet Safety Technical Task Force , at 13 (available at <a href="http://cyber.law.harvard.edu/research/isttf">http://cyber.law.harvard.edu/research/isttf</a> ) (last accessed May 13, 2009).....	12
Laura DeBonis, Technology Advisory Board Report (available at <a href="http://cyber.law.harvard.edu/research/isttf">http://cyber.law.harvard.edu/research/isttf</a> ) (last accessed May 13, 2009).....	12
Editorial, “ <u>Toughest</u> ” Isn’t Justice, Columbus Ledger – Enquirer, June 27, 2006.....	2, 22

This Court should declare unconstitutional and preempted the provisions of O.C.G.A. § 42-1-12 (the “Registration Act”) that require sex offender registrants to provide internet identifiers to law enforcement for use and potential public release.

### **FACTUAL BACKGROUND AND SUMMARY OF THE ARGUMENT**

Plaintiff is a sex offender.<sup>1</sup> He served his time but nevertheless remains virtually imprisoned and deprived of fundamental rights. *Id.* ¶ 3. Plaintiff maintains e-mail and other accounts to store communications and writings, and these accounts also permit him to initiate communications. *Id.* ¶¶ 10, 12, 15, 18-25. These accounts are the electronic equivalent of a locked desk. Within the drawers of this desk, plaintiff files his personal papers, effects and letters. E-mails contained in these drawers are written through accounts not publicly associated with the plaintiff. *Id.* ¶¶ 10-12. A username is associated with the accounts and disclosed publicly when materials are sent over the internet, but the relationship between plaintiff and a username is not public. *Id.* ¶¶ 15-19. Each of the drawers to this virtual desk is locked and accessible via a virtual key: plaintiff’s password. Although it is undisputed that the government could not compel plaintiff to turn over a key to his desk to permit the government to open the drawers and review their contents at will, that is exactly what Georgia law requires. These intangibles are part of plaintiff’s

---

<sup>1</sup> Ex. A, Declaration of Terrence J. White (“White Decl.”) ¶ 2.  
483476.1



personal papers and effects and are protected from abridgement, unlawful interference and unreasonable search and seizure.

In 2008, the General Assembly amended the Registration Act,<sup>2</sup> increasing the information to be disclosed with the intention that sex offenders' internet use would be "monitored, or limited."<sup>3</sup> Registrants must now disclose their e-mail addresses, usernames and passwords for accounts that offer e-mail or interactive forums,<sup>4</sup> even though the operative terms, including "username," "user password" and "interactive online forums" are vague and overly broad.<sup>5</sup> The sheriff then has 72 hours to transmit the information to the GBI (O.C.G.A. § 42-1-12(h)(1)), who then must transmit it to the FBI within 24 hours. O.C.G.A. § 42-1-12(h)(2). The sheriff and the GBI also may release a registrant's internet identifiers if they conclude, in their own judgment, that release will protect the public, an undefined standard. O.C.G.A. § 42-

---

<sup>2</sup> Ex. B, 2008 Ga. Laws p. 810 ("SB 474").

<sup>3</sup> Ex. C, Press Release, Georgia Senate, Model Internet Safety Legislation Passes Senate (Feb. 28, 2008). Stringent requirements have always been part of the Registration Act, with the purpose of encouraging sex offenders to leave Georgia: "If it becomes too onerous and too inconvenient, they just may want to live somewhere else. And I don't care where, as long as it's not in Georgia." Ex. D, Editorial, "Toughest" Isn't Justice, Columbus Ledger – Enquirer, June 27, 2006.

<sup>4</sup> See O.C.G.A. § 42-1-12(a)(16)(K).

<sup>5</sup> O.C.G.A. § 42-1-12(a)(21.1) ("user name" is "string of characters chosen to uniquely identify an individual who uses a computer or other device with Internet capability to communicate with other individuals through the exchange of e-mail or instant messages or by participating in interactive online forums"); § 42-1-12(a)(21.2) ("user password" is "string of characters that enables an individual that enables an individual who uses a computer or other device with Internet capability to gain access to e-mail messages and interactive online forums").

1-12(o). Failure to comply risks a sentence of 10-30 years or life.<sup>6</sup> These provisions (the “E-Information Provisions”), including the addition of e-mail addresses, usernames and user passwords; transmittal from sheriffs to the GBI and the FBI; the defendants’ ability to release it; and the penalties resulting from failure to disclose, are the subject of plaintiff’s challenge.

Plaintiff is required to register as a sex offender.<sup>7</sup> He frequently uses the internet and will be harmed if the E-Information Provisions are enforced. White Decl. ¶ 9. He maintains multiple e-mail accounts, accounts with social networking websites, online retailers, blogs and genealogy websites. *Id.* ¶¶ 10, 15, 18, 20-23. For some of these accounts, plaintiff uses his full legal name, and for others he uses a pseudonym, to send emails, post on blogs and chat. *Id.* ¶¶ 10-11, 13, 15, 17. Plaintiff’s accounts electronically store his communications and financial information. *Id.* ¶¶ 12, 20-23. The E-Information Provisions require him to provide the keys to his e-mail communications, including those with his legal counsel, and

---

<sup>6</sup> See O.C.G.A. § 42-1-12(n).

<sup>7</sup> Plaintiff now must register as a sex offender, but was not required to do so at the time of his offenses. He became subject to the Registry after serving a year for possessing marijuana in violation of his probation for the sex crime. White Decl. ¶¶ 7-8. Although his offenses were committed 10 years prior to the marijuana conviction, his release for the marijuana offense forced him to register. O.C.G.A. § 42-1-12(e). Plaintiff was not convicted of any criminal offense against a minor on or after July 1, 1996.

they permit the identification of plaintiff as the owner of the accounts.<sup>8</sup> If plaintiff must disclose his internet identifiers, law enforcement can access and monitor his accounts and communications without a warrant. Plaintiff does not consent to this access. White Decl. ¶¶ 25-26. Yet Georgia law exposes him to unfettered search, constructively seizing entire communications channels. Other courts have stricken similar laws. *See Doe v. Shurtleff*<sup>9</sup> (statute requiring sex offenders to provide usernames and passwords violates First Amendment); *Doe v. Prosecutor, Marion County, Ind.*<sup>10</sup> (statute requiring sex offenders to consent to searches of their computers violates Fourth Amendment.)

### **ARGUMENT AND CITATION OF AUTHORITY**

Plaintiff is entitled to the requested injunctive relief because:

(1) [he] has a substantial likelihood of success on the merits; (2) irreparable injury will be suffered unless the injunction issues; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) if issued, the injunction would not be adverse to the public interest. For a permanent injunction, the standard is essentially the same, except that the movant

---

<sup>8</sup> These broad provisions also require registrants to provide identifiers for bank and tax preparation accounts, telephone over internet websites and accounts for retailers of goods and services. Several financial and communications based websites create accounts with interactive capabilities and which would be required to be disclosed if used by a sex offender. *See, e.g.,* [www.turbotax.com](http://www.turbotax.com); [www.bellsouth.com](http://www.bellsouth.com); [www.suntrust.com](http://www.suntrust.com); [www.wachovia.com](http://www.wachovia.com); [www.skype.com](http://www.skype.com).

<sup>9</sup> No. 1:08-cv-64, 2008 WL 4427594 (D. Utah Sept. 25, 2008) (Ex. E).

<sup>10</sup> 566 F. Supp. 2d 862 (S.D. Ind. 2008) (Ex. F).

must establish actual success on the merits, as opposed to a likelihood of success.<sup>11</sup>

Plaintiff meets this burden and the Court should declare the E-Information Provisions preempted and unconstitutional and enjoin their enforcement.

## **I. Plaintiff Will Succeed On The Merits Of His Claims.**

### **A. The E-Information Provisions Are Preempted.**

The Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-11, preempts the E-Information Provisions.<sup>12</sup> The SCA prohibits unauthorized access to an electronic communication or a stored communication:

whoever (1) *intentionally accesses without authorization* a facility through which an electronic communication service is provided; or *intentionally exceeds an authorization* to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system *shall be punished* . . . .<sup>13</sup>

“A person violates the SCA if she accesses an electronic communication service, *or* obtains an electronic communication while it is still in electronic storage, without authorization.”<sup>14</sup> Thus, unauthorized access of information stored on or conveyed by

---

<sup>11</sup> *KH Outdoor, LLC v. Trussville*, 458 F.3d 1261, 1268 (11<sup>th</sup> Cir. 2006).

<sup>12</sup> “Congress’s intent to preempt state law may be explicitly stated in the language of a federal statute or implicitly contained in the structure and purpose of the statute. . . . [T]he Supreme Court has identified three types of preemption: (1) express preemption; (2) field preemption; and (3) conflict preemption.” *Cliff v. Payco Gen. Am. Credits Inc.*, 363 F.3d 1113, 1122 (11<sup>th</sup> Cir. 2004).

<sup>13</sup> 18 U.S.C. § 2701(a) (emphasis added).

<sup>14</sup> *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 483476.1

websites;<sup>15</sup> of e-mail or online accounts that save messages;<sup>16</sup> and of e-mails stored with a service provider after delivery<sup>17</sup> violate the SCA.<sup>18</sup>

The E-Information Provisions allow the very access prohibited by the SCA by providing law enforcement and, potentially, the public unfettered access to electronic communications.<sup>19</sup> Indeed, the Georgia legislature intended this law to permit “law enforcement to monitor a registered sex offenders’ online activity.” Ex. C. While the E-Information Provisions do not provide express authorization for public access to online accounts, law enforcement’s ability to *disclose* such information in order to “protect the public”<sup>20</sup> encourages and will result in unauthorized access in violation

---

(S.D.N.Y. 2008).

<sup>15</sup> *U.S. v. Steiger*, 318 F.3d 1039, 1047 (11<sup>th</sup> Cir. 2003) (data stored and conveyed on websites “falls within the definition of ‘electronic communications’”).

<sup>16</sup> *Pure Power*, 587 F. Supp. 2d at 560 (violation of SCA where employer obtained e-mails “located on, and accessed from third-party communication service provider systems”); *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) (summary judgment appropriate “where the facts indisputably present a case of an individual logging onto another’s e-mail account without permission and reviewing the material therein”); *but see Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (concluding without analysis or citation that SCA “does not prohibit...obtaining ‘opened’ e-mails”).

<sup>17</sup> *U.S. v. Councilman*, 418 F.3d 67, 79 (1<sup>st</sup> Cir. 2005) (en banc); *Pure Power*, 587 F. Supp. 2d 548 (emails on hotmail.com were stored communications).

<sup>18</sup> Forced disclosure of a username and password for the account does not necessarily confer “authorization.” *Pure Power*, 587 F. Supp. 2d at 562 (“At most one could argue that [the employee had] consented to [his employer] viewing his password. But he did not consent to her to [sic] using it.”).

<sup>19</sup> See O.C.G.A. §§ 42-1-12(h) (required registration information to be transmitted to GBI); *id.* § 42-1-12(o) (permitting disclosure of registration information).

<sup>20</sup> O.C.G.A. § 42-1-12(o).

of the SCA. By permitting the monitoring and disclosure of internet identifiers, the legislature is circumventing the SCA and effectively searching a registrant's electronic communications without authority (or a warrant).<sup>21</sup> Because "[t]he purpose of Congress is the ultimate touchstone"<sup>22</sup> of preemption and Congress intended to prohibit unauthorized access, the E-Information Provisions are preempted by field and conflict preemption.

### **1. The SCA Preempts The Stored Communications Field.**

Field preemption occurs when a federal law "so pervasively regulates in the field...that Congress left no room for states to supplement." *Cliff*, 363 F.3d at 1125. Several courts have held that the SCA preempts the field due to its broad language and pervasive regulatory scheme.<sup>23</sup> With the SCA, Congress created a comprehensive regulatory scheme. The SCA: (1) prohibits unauthorized access to

---

<sup>21</sup> That the SCA provides a defense to a party prosecuted in an action brought pursuant if she relied in good faith on legislative or statutory authorization does not permit the E-Information Provisions. *See* 18 U.S.C. § 2707(e). First, the existence of a defense does not make unlawful conduct lawful. It simply provides that the conduct cannot be the basis for an action. Second, the Georgia law is not a legislative or statutory authorization because it does not explicitly authorize access. Instead, it encourage and *implicitly* authorizes violation of the SCA and fails to provide necessary procedural safeguards to ensure that rights are not infringed.

<sup>22</sup> *Retail Clerks Int'l Ass'n, Local 1625 v. Schermerhorn*, 375 U.S. 96, 103 (1963).

<sup>23</sup> *See, e.g., Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1138 (C.D. Cal. 2006), *aff'd in part, rev'd in part*, 529 F.3d 892 (9<sup>th</sup> Cir 2008); *Muskovich v. Crowell*, No. 3-95-CV-80007, 1995 WL 905403, at \*1 (S.D. Iowa March 21, 1995); *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1155 (C.D. Cal. 2006) (Electronic Communications Privacy Act preempts field because it "is very comprehensive").

stored electronic communications (18 U.S.C. § 2701(a)); (2) creates a private right of action for violations (18 U.S.C. § 2707(a)); (3) creates specific standards regulating when the contents of stored electronic communications may be released (18 U.S.C. § 2702); (4) creates a comprehensive framework for obtaining the contents and records of stored communications (18 U.S.C. §§ 2703(a)-(c)), permitting access only upon authorization or when a warrant issues based upon “specific and articulable facts” (18 U.S.C. § 2703(d)); (5) requires notice before accessing or copying electronic communications (18 U.S.C. §§ 2703(b), 2704(a)(2), 2705); (6) creates a procedure for one whose electronic information is copied to challenge the order authorizing the taking (18 U.S.C. § 2704(b)); and (7) creates exclusive remedies for violations (18 U.S.C. § 2708). Moreover, because the SCA governs electronic communications, which is not “a field traditionally regulated by the states,” *Cliff*, 363 F.3d at 1125, a finding of field preemption is particularly warranted. Congress did not intend any state to occupy this field.

## **2. The E-Information Provisions Conflict With The SCA.**

Alternatively, the SCA preempts Georgia’s law because the law “stands as an obstacle to the accomplishment of Congress’s objectives in enacting the [SCA]” and conflicts with the SCA. *Id.* at 1127. The provisions provide the keys to access registrants’ accounts without permission, frustrating the SCA’s purpose of protecting the privacy of online communications. Registrants must disclose their internet

identifiers and permit the government to monitor their communications. Ex. C. Such unauthorized monitoring conflicts with the SCA, which only permits access with authorization or if procedures are followed to ensure that constitutional standards are met. Plaintiff has not, and does not, authorize access to his internet accounts. White Decl. ¶¶ 25-26. Nor has Georgia enacted procedures to ensure that access to accounts does not unlawfully infringe rights. The E-Information Provisions thus conflict with the SCA and are preempted.

**B. The Provisions Violate First Amendment Free Speech Rights.**

Plaintiff's First Amendment free speech rights are violated because the provisions deprive him of his right to anonymous speech, are a content-based prior restraint, do not meet the requirements of strict scrutiny, are overly broad and are impermissibly vague. Nearly identical provisions have been found to violate the First Amendment because they abridged sex offenders' rights to anonymous speech and were content-based restrictions, but not narrowly tailored to further the state's interest.<sup>24</sup> The E-Information Provisions suffer from the same infirmities, and this Court should also enjoin their enforcement.

**1. The Provisions Violate The Right to Anonymous Speech.**

Registrants, have a right to anonymous or speech, for any reason, including "fear of economic or official retaliation,...concern about social ostracism, or...a

---

<sup>24</sup> See *Shurtleff*, No. 1:08-cv-64, 2008 WL 4427594, at \*8.  
483476.1



desire to preserve as much of one's privacy as possible.”<sup>25</sup> Such speech is an integral part of our history and tradition,<sup>26</sup> and applies to the internet.<sup>27</sup> Indeed,

[t]hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.<sup>28</sup>

Because the E-Information Provisions remove a registrant's right to speak anonymously on the internet due to required disclosure of internet identifiers, the provisions unlawfully deprive plaintiff of his right to free speech.<sup>29</sup>

## 2. The Provisions Are Presumptively Invalid Content-Based Restrictions.

Because Georgia's law applies only to sex offenders, it is, as *Shurtleff* held, a content based restriction.<sup>30</sup> Georgia courts have agreed, finding that a “statute's

---

<sup>25</sup> *Watchtower Bible & Tract Soc'y of N.Y. v. Village of Stratton*, 536 U.S. 150, 166-67 (2002).

<sup>26</sup> *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (“Anonymity is a shield from the tyranny of the majority....exemplif[y]ing the purpose behind...the First Amendment...: to protect unpopular individuals from retaliation-and their ideas from suppression-at the hand of an intolerant society.”).

<sup>27</sup> *See Sinclair v. TubeSockTedD*, 596 F. Supp. 2d 128, 131 (D.D.C. 2009) (collecting cases recognizing the right to anonymous internet speech).

<sup>28</sup> *Reno v. ACLU*, 521 U.S. 844, 870 (1997).

<sup>29</sup> *See Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1091-93 (W.D. Wash. 2001) (removal of anonymity on internet chills internet communications); *Ashcroft v. ACLU*, 542 U.S. 656, 670-671(2004)( “Where a prosecution is a likely possibility, yet only an affirmative defense is available, speakers may self-sensor rather than risk the perils of trial. There is a potential for extraordinary harm and a serious chill upon protected speech.”).

<sup>30</sup> *Shurtleff*, No. 1:08-cv-64, 2008 WL 4427594, at \*8. *See also Solantic, LLC v. City* 483476.1

prohibition of internet transmissions which ‘falsely identify’ the sender constitutes a presumptively invalid content-based restriction.”<sup>31</sup> Requiring plaintiff to self-identify all names through which he communicates, coupled with long prison terms for noncompliance, is a presumptively invalid restriction that cannot stand unless defendants meet a high burden. As the Supreme Court held:

***Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard against that threat the Constitution demands that content-based restrictions on speech be presumed invalid and that the government bear the burden of showing their constitutionality.***<sup>32</sup>

To prevail, defendants “must demonstrate that the statute furthers a compelling state interest and is narrowly tailored to achieve it.”<sup>33</sup> They cannot do this because “the governmental interest in protecting children from harmful materials...does not justify an unnecessarily broad suppression of speech addressed to adults.”<sup>34</sup> The E-Information Provisions require disclosure of ***all*** internet identifiers for accounts with

---

*of Neptune Beach*, 410 F.3d 1250, 1265-66 (11<sup>th</sup> Cir. 2005) (regulations that “pick and choose the *speakers* entitled to preferential treatment are no less content based than those that select among subjects or messages.”); *ACLU v. Miller*, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997) (enjoining Georgia law prohibiting fictitious names in e-mail or websites as a content-based regulation).

<sup>31</sup> *Miller*, 977 F. Supp. at 1232.

<sup>32</sup> *Ashcroft v. ACLU*, 542 U.S. 656, 661 (2004) (emphasis added).

<sup>33</sup> *Miller*, 977 F.Supp. at 1232 (citing *Sable Communs. of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989)).

<sup>34</sup> *Reno*, 521 U.S. at 875.

“interactive online forums.”<sup>35</sup> This includes accounts where there is little to no risk of contact with children, such as bank, retail, genealogy and blog accounts.<sup>36</sup> The law does not meet its alleged purpose of protecting children because it does not apply outside Georgia.<sup>37</sup> Moreover, registrants are not the only threat to children on the internet.<sup>38</sup> Nor is there data showing that regulations like the E-Information Provisions are effective.<sup>39</sup> Finally, less restrictive alternatives are available, such as a search warrant or subpoena to a registrant’s internet service provider.<sup>40</sup> The Supreme Court has also outlined less restrictive means: Georgia can “enact[] programs to promote use of filtering software” to “give parents that ability [to monitor their children’s access] without subjecting protected speech to severe penalties.”<sup>41</sup>

---

<sup>35</sup> O.C.G.A. §§ 42-1-12(a)(21.1)-(21.2).

<sup>36</sup> White Decl. ¶¶ 10, 15, 17-20.

<sup>37</sup> Under this law, a sex offender outside Georgia, in another state, could still chat anonymously with a child in Georgia over the internet. *See Ashcroft*, 542 U.S. at 667-68 (2004) (statute targeting child pornography created in America “does not prevent minors from having access to those harmful materials....It is not an answer to say that COPA reaches some amount of materials that are harmful to minors; the question is whether it would reach more of them than less restrictive alternatives”).

<sup>38</sup> Ex. G, Laura DeBonis, Technology Advisory Board Report, at 15 (“Not all potential problem users have been previously identified or registered in the sex offender database or other watchlists; thus, a system relying on such data will be inherently limited.”).

<sup>39</sup> Ex. H, Andrew Schrock & danah boyd, Online Threats to Youth: Solicitation, Harassment, and Problematic Content: Literature Review Prepared for the Internet Safety Technical Task Force, at 13 (available at <http://cyber.law.harvard.edu/research/isttf>) (last accessed May 13, 2009).

<sup>40</sup> *See Shurtleff*, 2008 WL 4427594, at \* 9.

<sup>41</sup> *Ashcroft*, 542 U.S. at 670.

### 3. The E-Information Provisions Are A Prior Restraint.

A regulation like Georgia's that requires individuals to obtain permission before speaking is a prior restraint.<sup>42</sup> Thus, a requirement that protestors pass through a metal detector before protesting was an unconstitutional prior restraint because it did not provide for "meaningfully judicial review prior to the end of the protest." *Id.* Similarly, a registrant has no way to seek review before disclosing his internet identifiers or before they are disclosed to others. Instead, he must pass under an intrusive screening device that connects him to his speech and distributes his information at will.<sup>43</sup> This prior restraint is unconstitutional.<sup>44</sup>

### 4. The E-Information Provisions Are Overly Broad.

---

<sup>42</sup> *Bourgeois v. Peters*, 387 F.3d 1303, 1319 (11<sup>th</sup> Cir. 2004).

<sup>43</sup> See O.C.G.A. §§ 42-1-12(f)(5); 42-1-12(o).

<sup>44</sup> The lack of procedures for review prior to distribution of internet identifiers to the public also violates the Fourteenth Amendment's equal protection and procedural due process clauses. The E-Information Provisions also impermissibly impact a suspect class, sex offenders, solely due to their classification as such, and "interfere[] with the exercise of a fundamental right." *Provident Mut. Life Ins. Co. v. Atlanta*, 864 F.Supp. 1274, 1291 (N.D. Ga. 1994). Of the fundamental rights identified by the Supreme Court, four are implicated by the E-Information Provisions: "the right to freedom of association; ...the right to fairness in the criminal process; ...the right to procedural due process; and...the right to privacy." *Id.* As discussed more fully herein, plaintiff's rights of free association, procedural due process and privacy are all infringed. Plaintiff's right to fairness in criminal proceedings is also infringed because the provisions permit law enforcement to access communications with legal counsel. Defendants do not meet their burden because the E-Information Provisions are not narrowly tailored.

The E-Information Provisions are overly broad because they ““sweep[] protected activity within [their] proscription” and “ha[ve] the potential to chill the expressive activity of others not before the court.”<sup>45</sup> For example, although plaintiff is entitled to privately conduct banking activities online, the provisions require that he disclose his username and password for any such account. If he worked in a profession requiring the maintenance of privacy, such as the law or medicine, he would be required to violate his professional responsibilities and permit access to protected communications. These examples have no relationship to the protection of children, but still must be disclosed because they permit a to communicate with others. The E-Information Provisions

w[ere] not drafted with the precision necessary for laws regulating speech. On its face, the act prohibits such protected speech as the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy...Therefore, even if the statute could constitutionally be used to prosecute persons who intentionally [fail to register] the statute is nevertheless overbroad because it operates unconstitutionally for a substantial category of the speakers it covers.<sup>46</sup>

Moreover, the ability of law enforcement alone to determine whether disclosure of internet identifiers “is necessary to protect the public”<sup>47</sup> illustrates a lack of clear

---

<sup>45</sup> *Miller*, 977 F.Supp. at 1233 (internal citations omitted).

<sup>46</sup> *Id.*

<sup>47</sup> O.C.G.A. §§ 42-1-12(o)(1),(3).

483476.1

standards which creates the “risk of discriminatory enforcement” and “poses great[] First Amendment concerns.”<sup>48</sup> These provisions should be enjoined.

### **5. The E-Information Provisions Are Void For Vagueness.**

The E-Information Provisions are void because they fail “to ‘define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.’”<sup>49</sup> As one example, the term “interactive online forum” includes any web-based account through which a communication can be made, including financial accounts. Moreover, if an account plaintiff currently possesses adds interactive capabilities, does he violate the law for failing to update his registration within 72 hours? How is he to know when the clock starts ticking? When Georgia attempted to make criminal the use of false names in e-communications, the *Miller* court held that “the statute is void for vagueness because it 1) does not give fair notice of the scope of conduct it proscribes; 2) is conducive to arbitrary enforcement; and 3) infringes upon plaintiffs’ free expression.”<sup>50</sup> This court should likewise hold.

### **C. The E-Information Provisions Infringe Private Association.**

---

<sup>48</sup> *Reno*, 521 U.S. at 872.

<sup>49</sup> *Miller*, 977 F.Supp. at 1234. Because plaintiff will cease communications rather than risk disclosure, White Decl. ¶¶ 27-28, “the policies underlying the vagueness rule apply with special force.” *Miller*, 977 F. Supp. at 1234.

<sup>50</sup> *Miller*, 977 F.Supp. at 1234.

Plaintiff's right to freedom in his associations,<sup>51</sup> including the right to engage in such associations anonymously,<sup>52</sup> is unconstitutionally infringed because the law chills his speech by forcing disclosure of every forum where he may interact with others. Thus, where groups are compelled to disclose membership lists, the Supreme Court has found First Amendment violations.<sup>53</sup> Georgia has no compelling interest in prohibiting plaintiff's right to anonymously associate with groups on the internet.<sup>54</sup> As discussed in Section I-B-2 above, defendants cannot show that these provisions redress any harm. And, there are less restrictive means for addressing any conjectural harm than infringing plaintiff's association rights. Moreover, where, as

---

<sup>51</sup> *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960) ("freedom of association for the purpose of advancing ideas and airing grievances is protected by the Due Process Clause of the Fourteenth Amendment from invasion by the States."); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460-61 (1958) ("freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."); *Gibson v. Florida Legislative Investigation Committee*, 372 U.S. 539, 543 (1963) ("This Court has repeatedly held that rights of association are within the ambit of the constitutional protections afforded by the First and Fourteenth Amendments.").

<sup>52</sup> *NAACP*, 357 U.S. at 462 (there is a "vital relationship between freedom to associate and privacy in one's associations"); *Gibson*, 372 U.S. at 544 ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.").

<sup>53</sup> *See NAACP*, 357 U.S. at 449 (order requiring NAACP to produce membership lists held unconstitutional as violative of fundamental rights to association).

<sup>54</sup> *Bates*, 361 U.S. at 524 ("Where there is a significant encroachment upon personal liberty, the State may prevail only upon showing a subordinating interest which is compelling.").

here,<sup>55</sup> there is “evidence that fear of community hostility and economic reprisals that would follow public disclosure of the membership lists had discouraged new members from joining the organizations and induced former members to withdraw,” the offending statute violates the First Amendment.<sup>56</sup> Because some groups through which plaintiff associates may involve unpopular views, the protection of anonymous association is all the more necessary:

where the challenged privacy is that of persons espousing beliefs already unpopular with their neighbors [] the deterrent and ‘chilling’ effect on the free exercise of constitutionally enshrined rights of free speech, expression, and association is consequently the more immediate and substantial.<sup>57</sup>

Sex offenders’ right to associate is unconstitutionally infringed by the Georgia law.

#### **D. The E-Information Provisions Violate the Fourth Amendment.**

The Supreme Court has held that “[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.”<sup>58</sup> In Georgia, that maxim does not apply: registrants’ accounts may be searched and constructively seized without probable cause, a warrant or judicial review.

##### **1. The Fourth Amendment Bars Searches Without A Warrant.**

---

<sup>55</sup> White Decl. ¶¶ 27-29.

<sup>56</sup> *Bates*, 361 U.S. at 524.

<sup>57</sup> *Gibson*, 372 U.S. at 556-57.

<sup>58</sup> *Katz v. U.S.*, 389 U.S. 347 (1967).



“A search occurs when ‘an expectation of privacy that society is prepared to consider reasonable is infringed.’”<sup>59</sup> The property searched here is the plaintiff’s electronic accounts, which are subject to the same privacy expectation as their tangible counterparts, letters and written papers.<sup>60</sup> The E-Information Provisions require plaintiff to make public and disclose the usernames and e-mail addresses he uses to communicate online,<sup>61</sup> many of which are pseudonyms that he has previously chosen to keep private and would not otherwise disclose,<sup>62</sup> but the law requires he must disclose the key to access each of these accounts.<sup>63</sup> Because law enforcement can use plaintiff’s internet identifiers for any “law enforcement purpose” and can distribute them if disclosure will “protect the public,” a search occurs.<sup>64</sup> But, no warrant or finding of probable cause must be made prior to accessing accounts. This warrantless search is unconstitutional:

---

<sup>59</sup> *Maryland v. Macon*, 472 U.S. 463, 469 (1985) (internal citation omitted).

<sup>60</sup> *U.S. v. Forrester*, 512 F.3d 500, 511 (9<sup>th</sup> Cir. 2008) (“E-mail, like physical mail, has an outside address ‘visible’ to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical.”); *U.S. v. Finley*, 477 F.3d 250, 259 (5<sup>th</sup> Cir. 2007) (“reasonable expectation of privacy in the call records and text messages on the [non-password protected] cell phone” provided by employer); *Quon*, 529 F.3d at 905 (“reasonable expectation of privacy in the content of their text messages.”).

<sup>61</sup> O.C.G.A. § 42-12-1(f).

<sup>62</sup> White Decl. ¶¶ 10-11; 15-20.

<sup>63</sup> O.C.G.A. § 42-1-12(a)(21.2).

<sup>64</sup> One of the legislature’s goals was to ensure that electronic communications could be monitored. Ex. C. The provisions are intended render private information public such that warrants are no longer required prior to a search.

Searches conducted without warrants have been held unlawful “notwithstanding facts unquestionably showing probable cause,” for the Constitution requires “that the deliberate, impartial judgment of a judicial officer be interposed between the citizen and the police.”<sup>65</sup>

Convicted sex offenders have the same rights to privacy and to be free from unreasonable searches as other citizens: “A person’s status as a felon who is no longer under any form of punitive supervision therefore does not permit the government to search his home and belongings without a warrant.” *Doe*, 566 F.Supp.2d at 883. A similar scheme requiring sex offenders to consent to electronic searches at any time “violate[d] the plaintiffs’ Fourth Amendment rights.”<sup>66</sup>

---

<sup>65</sup> *Katz* 389 U.S. at 357 (internal citations omitted). *See also Quon*, 529 F.3d at 908 (employer’s search in content of employee’s texts on employer-provided device unreasonable absent warrant). The provisions are a writ of assistance because they provide access to plaintiff’s communications at any time and for any reason. *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (“These words...reflect the determination of those who wrote the Bill of Rights that ***the people of this new Nation should forever ‘be secure in their persons, houses, papers and effects’ from intrusion and seizure by officers acting under the unbridled authority of a general warrant.*** Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance...***The hated writs of assistance had given customs officers blanket authority to search where they pleased*** for goods imported in violation of the British tax laws. ***They were denounced*** by James Otis as ‘the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book,’ ***because they placed ‘the liberty of every man in the hands of every petty officer.’***”)(emphasis added).

<sup>66</sup> *Id.* at 878. The *Doe* court expressed concern with the breadth of the searches: “The parties have not cited, and the court has not found, any American law that attempts to authorize such a broad intrusion on personal privacy and security, without a warrant, probable cause, or even reasonable suspicion, for persons not in prison or subject to parole, probation, or other court supervision.” *Id.* In *Doe*, a registrant was required to permit searches of his electronic communications devices. Moreover, he was

## 2. The E-Information Provisions Are A Constructive Seizure.

“A seizure occurs when ‘there is some meaningful interference with an individual’s possessory interests’ in the property seized.”<sup>67</sup> The E-Information Provisions constitute a **constructive** seizure<sup>68</sup> because they force plaintiff to cease some electronic communications and writings or face a felony conviction for failing to disclose internet identifiers, foreclosing and appropriating an entire channel of communications.<sup>69</sup> They are therefore a content based prior restraint on plaintiff’s speech,<sup>70</sup> and “First Amendment concerns not raised by other kinds of seizures” are implicated, such that “certain special conditions be met before such seizures may be carried out.”<sup>71</sup> Indeed, because “*there is a strong presumption against* the constitutional validity” of a prior restraint, “*greater procedural safeguards must be*

---

required to install hardware to monitor computer usage. There is no difference in the effect of the Indiana and Georgia laws, however. Both require registrants to effectively consent to searches of electronic communications at any time. And the Georgia law goes further – it does not require **actual** consent and it permits law enforcement to enable others, including the general public, to have the keys to electronic information.

<sup>67</sup> *Macon*, 472 U.S. at 469 (citing *U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984)).

<sup>68</sup> *Penthouse Int’l, Ltd. v. McAuliffe*, 610 F.2d 1353, 1360 (5<sup>th</sup> Cir. 1980) (“The distributors and retailers, by reason of intimidation and the threat of prosecution, were caused to cease selling the ‘suspect’ publications” which “effected a ‘constructive seizure’ of the complainant’s publications”).

<sup>69</sup> White Decl. ¶¶ 27-28.

<sup>70</sup> See Section I-B-2, above.

<sup>71</sup> *New York v. P.J. Video, Inc.*, 475 U.S. 868, 873 (1986).

*afforded before the occurrence of a ‘constructive seizure.’”*<sup>72</sup> Thus, seizures of obscene materials are unconstitutional where police determine obscenity with no review by a neutral magistrate before or after the seizure.<sup>73</sup> The E-Information Provisions do not provide for any judicial review prior to or after seizing plaintiff’s internet identifiers and thus violate the Fourth Amendment.

Moreover, law enforcement can seize plaintiff’s electronic communications essentially forever without ever obtaining a search warrant or returning the right of sole access to plaintiff. The Eleventh Circuit recently held that seizing property without timely obtaining a warrant violates the Fourth Amendment.<sup>74</sup> In *Mitchell*, federal agents seized a hard drive, but did not obtain a search warrant for 21 days, which “constitute[d] a significant interference with [the owner’s] possessory interest” even though probable cause existed. *Id.* at \*3. The court held that a hard drive “‘is

---

<sup>72</sup> *Penthouse Int’l.*, 610 F.2d 1361 (emphasis added).

<sup>73</sup> *See Roaden v. Kentucky*, 413 U.S. 496, 504 (1973) (“***The seizure is unreasonable***, not simply because it would have been easy to secure a warrant, but rather because ***prior restraint of the right of expression***, whether by books or films, ***calls for a higher hurdle in the evaluation of reasonableness***. The setting of the bookstore or the commercial theater, each presumptively under the protection of the First Amendment, invokes such Fourth Amendment warrant requirements because ***we examine what is ‘unreasonable’ in the light of the values of freedom of expression.***”) (emphasis added); *Penthouse Int’l.*, 610 F.2d at 1361 (prior restraint constituting constructive seizures may be constitutional if it “involves ***the requirement of a judicial determination*** of some type by a neutral detached magistrate either ***before or immediately after the seizure*** of allegedly obscene material.”) (emphasis added).

<sup>74</sup> *U.S. v. Mitchell*, \_\_\_ F.3d \_\_\_, 2009 WL 1067212 (11<sup>th</sup> Cir. Apr. 22, 2009).

the digital equivalent of its owner's home, capable of holding a universe of private information.'" *Id.* at \*4. Similarly, Georgia permits seizure of "the digital equivalent of [plaintiff's] house." The difference is that plaintiff's property will never be returned: Unless the law is enjoined, he will regain control of his intangible property.

### **E. E-Information Provisions Are An Ex Post Facto Law.**

The E-Information Provisions are punitive in intent and an ex post facto law<sup>75</sup> because they punish sex offenders for their status, force them to relinquish their rights or face considerable jail time, and are intended to monitor their internet use.<sup>76</sup> Law enforcement oversees the provisions, as part of the "Penal Institutions" code section.<sup>77</sup> Finally, enticing a child for indecent purposes carries *exactly the same penalty* as a first violation of the Registry Act. *See* O.C.G.A. § 16-6-5.

---

<sup>75</sup> *Smith v. Doe*, 538 U.S. 84, 92 (2004) ("If the intention of the legislature was to impose punishment, that ends the inquiry. If, however, the intention was to enact a regulatory scheme that is civil and nonpunitive, we must further examine whether the statutory scheme is so punitive either in purpose or effect as to negate the State's intention to deem it 'civil.'") (internal citations omitted). Although the Supreme Court has held that a registration scheme was not an ex post facto law, *Smith*, 538 U.S. 84, the court did not consider provisions as broad or punitive as Georgia's, which infringe fundamental First and Fourth Amendment rights. And, the penalty for violation in *Smith* was a misdemeanor versus 10-30 years or life.

<sup>76</sup> Ex. C. In enacting the overall registration scheme, one legislator expressed punitive intent: "If it becomes too onerous and too inconvenient, they just may want to live somewhere else." Ex. D.

<sup>77</sup> A provision's location in a state's scheme or the persons charged with enforcing it evidence intent. In *Smith*, because the agency enforced civil and criminal laws, the intent was not punitive. 538 U.S. at 96. Here, however, the main responsibility of the sheriffs and the GBI is to enforce criminal laws.

Even if punitive intent did not exist, the law is punitive in effect.<sup>78</sup> It resembles traditional forms of punishment because it shames due to status<sup>79</sup> and banishes registrants from the internet or Georgia.<sup>80</sup> It is an affirmative disability and restraint because registrants must choose between sacrificing fundamental rights or imprisonment.<sup>81</sup> An affirmative disability also results because changes must be reported in 72 hours, requiring frequent and lengthy trips to the sheriff whenever an account is acquired or changed.<sup>82</sup> The harsh penalties for failure to comply, the risk of identifiers being disclosed and the lifelong registration term are also retributive and meant to deter crime.<sup>83</sup> Finally, the provisions are excessive: they require disclosure of identifiers whether or not children are involved.<sup>84</sup>

## **II. Plaintiff Faces A Substantial Threat Of Irreparable Injury.**

---

<sup>78</sup> “Whether the sanction involves an affirmative disability or restraint, whether it has historically been regarded as a punishment, whether it comes into play only on a finding of scienter, whether its operation will promote the traditional aims of punishment-retribution and deterrence, whether the behavior to which it applies is already a crime, whether an alternative purpose to which it may rationally be connected is assignable for it, and whether it appears excessive in relation to the alternative purpose assigned are all relevant to the inquiry [of whether a law is punitive in effect].” *Kennedy v. Mendoza-Martinez*, 372 U.S.144, 168-69 (1963).

<sup>79</sup> *Smith*, 538 U.S. at 97-98.

<sup>80</sup> *Doe v. Miller*, 405 F.3d 700, 719 (8<sup>th</sup> Cir. 2005) (banishment is a traditional punishment).

<sup>81</sup> *Id.* at 720 (restrictive laws “more likely to be” punitive).

<sup>82</sup> White Decl. ¶ 32. In contrast, registration does not constitute an affirmative disability where in person registration is not required. *Smith*, 538 U.S. at 101.

<sup>83</sup> *See Kansas v. Hendricks*, 521 U.S. 346, 362 (1997) (law is retributive when it “affix[es] culpability for prior criminal conduct”).

<sup>84</sup> *See* Section I-B-2 above.

“The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.”<sup>85</sup> In the Eleventh Circuit: “[t]he only area of constitutional jurisprudence where we have said that an on-going violation constitutes irreparable injury is the area of first amendment and right of privacy jurisprudence.”<sup>86</sup> And, where, as here, “failure to enjoin enforcement of [an] act will force plaintiff[] either to continue self-censorship or to risk criminal prosecution” he has “demonstrated a substantial threat of irreparable injury.”<sup>87</sup>

### **III. The Balance of Hardships Weighs In Plaintiff’s Favor.**

The balance of hardships weighs in plaintiff’s favor: “a temporary infringement of First Amendment rights constitutes a serious and substantial injury, and the [defendants] ha[ve] no legitimate interest in enforcing an unconstitutional [law].”<sup>88</sup> And, since defendants will claim that they cannot currently use the identifiers, they cannot suffer any harm if the information is not provided to them.

### **IV. The Issuance Of An Injunction Promotes the Public Interest.**

---

<sup>85</sup> *KH Outdoor*, 458 F.3d at 1271 (internal citation omitted).

<sup>86</sup> *Id.* at 1272 (citing *Northeastern Fla. Chapter of the Ass’n of Gen. Contractors of Am. v. City of Jacksonville*, 896 F.2d 1283, 1285 (11<sup>th</sup> Cir. 1990)).

<sup>87</sup> *Miller*, 977 F.Supp. at 1235.

<sup>88</sup> *KH Outdoor*, 458 F.3d at 1272 (11<sup>th</sup> Cir. 2006).

“No long string of citations is necessary to find that the public interest weighs in favor of having access to a free flow of constitutionally protected speech.”<sup>89</sup> “The public has no interest in enforcing an unconstitutional [law].”<sup>90</sup>

Respectfully submitted this 18<sup>th</sup> day of May, 2009.

/s/ Nicole G. Iannarone  
Emmet J. Bondurant  
Georgia Bar No. 066900  
Nicole G. Iannarone  
Georgia Bar No. 382510  
Elizabeth G. Eager  
Georgia Bar No. 644007

BONDURANT, MIXSON & ELMORE, LLP  
3900 One Atlantic Center  
1201 West Peachtree Street, N.W.  
Atlanta, Georgia 30309  
Telephone: 404-881-4100  
Facsimile: 404-881-4111  
E-mail: bondurant@bmelaw.com  
iannarone@bmelaw.com  
eager@bmelaw.com

*Attorneys for Plaintiff*

---

<sup>89</sup> *Miller*, 977 F.Supp. at 1235.

<sup>90</sup> *KH Outdoor*, 458 F.3d at 1272.



**CERTIFICATE OF COMPLIANCE**

Pursuant to Local Rule 7.1D of the Local Rules for the District Court for the Northern District of Georgia, I hereby certify that the foregoing pleading has been prepared in Times New Roman, 14 point font, as permitted by Local Rule 5.1B.

Respectfully submitted this 18<sup>th</sup> day of May, 2009.

/s/ Nicole G. Iannarone  
Nicole G. Iannarone  
Georgia Bar No. 382510

**CERTIFICATE OF SERVICE**

I, Elizabeth G. Eager, do hereby certify that I have this day electronically filed the foregoing MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR PRELIMINARY AND PERMANENT INJUNCTION AND DECLARATORY RELIEF with the Clerk of Court using the CM/ECF system which will automatically send email notification of such filing to the following attorneys of record:

Joseph Drolet, Esq.  
Paige Boorman, Esq.  
Office of the Attorney General  
40 Capitol Square  
Atlanta, Georgia 30334

In addition, I have served a copy upon the following individuals by United States mail, with adequate postage thereon and addressed as follows:

Governor Sonny Perdue  
100 Washington Street  
Atlanta, Georgia 30334

Thurbert Baker, Attorney General of Georgia  
40 Capitol Square SW  
Atlanta, Georgia 30334

Vernon Keenan  
Director of the Georgia Bureau of Investigations  
3121 Panthersville Road  
Decatur, Georgia 30034

Winston Denmark, Esq.  
Fincher Denmark & Williams LLC

2262 Mount Zion Road  
Jonesboro, Georgia 30236  
(Counsel for Tracy Graham-Lawson and Kem Kimbrough)

This 18th day of May, 2009.

/s/ Elizabeth G. Eager  
Elizabeth G. Eager  
Georgia Bar 644007